(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 29 43 436 A 1**

(51) Int. Cl. ³:
G 06 K 19/08
G 07 C 9/00
G 07 D 7/00
B 44 F 1/12
B 41 M 3/14

(21) Aktenzeichen: P 29 43 436.4-53
(22) Anmeldetag: 26. 10. 79
(43) Offenlegungstag: 7. 5. 81

(71) Anmelder:
Szepanski, Wolfram, Dr.-Ing., 5100 Aachen, DE

(72) Erfinder:
gleich Anmelder

(54) **Maschinell prüfbares Schutzmuster für Dokumente und Verfahren zur Erzeugung und Prüfung des Schutzmusters**

DE 29 43 436 A 1

DE 29 43 436 A 1

2943436

Patentansprüche

1. Druckfähiges Schutzmuster zum Fälschungsschutz von Dokumenten, das sowohl eine visuelle als auch eine maschinelle Echtheitsprüfung erlaubt, dadurch gekennzeichnet, daß eine flächig verspreizte Echtheitsinformation im Schutzmuster enthalten ist.

2. Schutzmuster nach Anspruch 1., dadurch gekennzeichnet, daß die Echtheitsinformation aus einem kodierten alfanumerischen Text besteht.

3. Schutzmuster nach Anspruch 2., dadurch gekennzeichnet, daß der alfanumerische Text ganz oder teilweise aus der individuellen Informationen (2) besteht, durch die sich zwei Dokumente gleicher Art unterscheiden.

4. Schutzmuster nach einem der Ansprüche 2. und 3., dadurch gekennzeichnet, daß der alfanumerische Text binär kodiert ist.

5. Schutzmuster nach einem der Ansprüche 1. bis 4., dadurch gekennzeichnet, daß die Verspreizung der Echtheitsinformation durch aneinandergefügte Flächenmuster (3) geschieht, die sich in ihren optischen Eigenschaften im Bereich des sichtbaren und / oder unsichtbaren Lichts unterscheiden.

6. Schutzmuster nach einem der Ansprüche 1. bis 5., dadurch gekennzeichnet, daß es aus unterschiedlichen zueinander orthogonalen oder bipolaren Flächenmustern (3), insbesondere Walsh- oder Karhunen-Loève Basisfunktionen zusammengesetzt ist.

7. Schutzmuster nach einem der Ansprüche 1. bis 6., dadurch gekennzeichnet, daß es sich auf einer transparenten Kunststoffolie befindet, die mit aggressivem Klebstoff unter Druck und Hitze auf die zu schützenden Oberflächen des Dokuments gebracht wird.

8. Schutzmuster nach einem der Ansprüche 1. bis 6., dadurch gekennzeichnet, daß es direkt auf das zu schützende Dokument gedruckt wird.

9. Schutzmuster nach Anspruch 8., dadurch gekennzeichnet, daß das zu schützende Dokument eine Banknote, ein Scheck oder ein Wertpapier ist.

10. Schutzmuster nach Anspruch 7. und 8., dadurch gekennzeichnet, daß das zu schützende Dokument ein Paßbild oder ein Ausweis ist.

11. Verfahren zur Echtheitsprüfung des Schutzmusters nach einem der Ansprüche 1. bis 10. mit Hilfe der Korrelationsdetektion, dadurch gekennzeichnet, daß die Korrelation mit einem Digitalrechner ausgeführt wird.

12. Verfahren zur Echtheitsprüfung des Schutzmusters nach einem der Ansprüche 1. bis 10., dadurch gekennzeichnet, daß eine Anordnung zur optischen Korrelation benutzt wird.

13. Verfahren zur Erzeugung eines Schutzmusters nach einem der Ansprüche 1. bis 10. dadurch gekennzeichnet, daß ein Digitalrechner benutzt wird, um das Schutzmuster auf das Dokument anzupassen und das Dokument selbst oder eine Druckmatrize hierfür herzustellen.

2943436

Dr.-Ing. Wolfram Szepanski
Harbachtalstraße 21
5100 Aachen

Maschinell prüfbares Schutzmuster für Dokumente und Verfahren zur Erzeugung und Prüfung des Schutzmusters

Die Erfindung bezieht sich auf ein maschinell prüfbares Schutzmuster für Dokumente, das eine über die Fläche des Dokuments verspreizte Echtheitsinformation enthält, sowie auf Verfahren zur Erzeugung des Schutzmusters und zu seiner Echtheitsprüfung.

Unter dem Begriff "Dokument" sollen hier Pässe, Identitätskarten, Berechtigungsausweise, Kreditkarten, Schecks, Banknoten, Wertpapiere und dgl. verstanden werden. Aufgrund der weiten Verbreitung dieser Dokumente und der mit ihnen verbundenen Werte wurden bereits verschiedene Maßnahmen zum Schutz vor Nachahmungen, Radierungen und sonstigen Verfälschungen angewendet. Als besonders sicher können Dokumente gelten, deren Echtheitsmerkmale nur schwer kopierbar oder verfälschbar sind und deren Unverfälschtheit auf verschiedene, von einander unabhängige Weisen und mit geringem Aufwand geprüft werden können. Dabei sollte der Fälschungsschutz vorzugsweise eine einfache visuelle Echtheitsprüfung erlauben, er sollte jedoch auch für eine maschinelle Prüfung durch automatische Lesegräte geeignet sein, um eine zweite, von der visuellen Prüfung unabhängige Kontrolle zu ermöglichen. Darüberhinaus eignen sich maschinell prüfbare Dokumente als Zahlungsmittel für Verkaufs- oder Geldwechselautomaten, als Ausweise für automatische Zugangskontrollen usw. und überall dort, wo eine große Anzahl von Dokumenten wie z. B. Banknoten oder Schecks maschinell registriert, sortiert oder gezählt werden muß. Gegenstand der Erfindung sind deshalb ebenfalls ein Verfahren zur Herstellung von geschützten Dokumenten sowie Verfahren zu ihrer maschinellen Echtheitsprüfung.

Um Nachahmungen zu erschweren und Fälschungen leicht kenntlich zu machen, werden Dokumente vielfach mit einem Schutzmuster überzogen. Am häufigsten verwendet werden komplizierte Linienmuster (Guillochen), die zwar eine visuelle Echtheitsprüfung erlauben, die aber in der Regel nicht maschinell lesbar sind. Dasselbe gilt für Schutzmuster mit einer dreidimensionalen optischen Wirkung, für die in den Auslege- und Offenlegungsschriften (DE-AS 23 34 702 bzw. DT-OS 26 03 558) keinerlei Hinweise auf eine maschinelle Prüfbarkeit gegeben werden.

Weiter sind Verfahren zum Dokumentenschutz bekannt, die auf dem Grundgedanken basieren, daß bestimmte maschinell lesbare Informationen oder Markierungen für einen Fälscher unsichtbar auf einem Dokument angebracht oder in ihm verborgen sind. Dies kann zum Beispiel durch die Verwendung von Materialien mit bestimmten elektrischen, magnetischen oder optischen Eigenschaften erzielt werden. Ein derartiger Dokumentenschutz ist nicht ohne Meßgeräte nachweisbar und kann ohne zusätzliche Maßnahmen auch nicht visuell überprüft werden. Wird die Existenz der unsichtbaren Markierung von einem Fälscher aber dennoch erkannt, so besteht die Gefahr einer Fälschung oder Nachahmung.

Es wurde auch ein Radierschutz vorgeschlagen (DT-AS 25 30 905), bei dem das Dokument von einer homogenen, informationslosen Schutzschicht bedeckt ist, die sich in ihren optischen Eigenschaften von der Informationsdruckfarbe und vom Papier unterscheidet und die Radierversuche in einem Lesegerät sichtbar werden läßt. Nicht erfaßt werden durch dieses Verfahren alle die Fälschungen, die ohne Radierungen dadurch zustande kommen, daß z. B. im Klartext auf das Dokument geschriebene Namensangaben oder Zahlenwerte durch Hinzufügen von Buchstaben oder Ziffern verändert werden.

Es ist ferner bekannt, sehr fälschungssichere Dokumente dadurch zu erzeugen, daß man eine Echtheitsinformation in Form eines Hologramms (DT-AS 25 01 604 und DT-AS 25 46 007) oder eines in Kunststoff eingeprägten, optischen Beugungsgitters (DT-AS 25 55 214) auf einem Dokument anbringt. Ein schwieriges, ungelöstes Problem

ist dabei die Erzeugung von kratz-, knick- und knitterfesten Hologrammen für Schecks und Banknoten, die gleichzeitig dünn, hochflexibel und dauerhaft abnutzungsfest sein müssen. Da die bekannten holographisch gesicherten Dokumente entweder ganz oder wenigstens an ihrer Oberfläche aus Kunststoff bestehen, können außerdem Schwierigkeiten entstehen, wenn die Dokumente nachträglich beschriftet oder gestempelt werden sollen. Bei der Massenherstellung von Dokumenten wirken sich die hohen Herstellungskosten für Hologramme zusätzlich nachteilig aus.

Aufgrund der genannten Mängel sind die bisher bekannten Verfahren des Dokumentenschutzes für bestimmte Arten von Dokumenten entweder garnicht oder nicht ökonomisch anwendbar oder sie erfüllen ihre Schutzfunktion nur unzureichend. Aufgabe der vorliegenden Erfindung ist es deshalb, einen maschinell prüfbaren Fälschungsschutz für Dokumente anzugeben, der in einer bevorzugten Ausführung auch eine visuelle Echtheitsprüfung erlaubt, und der bei allen eingangs definierten Dokumenten anwendbar ist, ohne die genannten Nachteile bisher bekannter Schutzmethoden zu besitzen. Es ist ferner Aufgabe der Erfindung, Verfahren anzugeben, mit denen die Herstellung des Schutzes sowie seine maschinelle Prüfung möglich ist.

Die Grundidee zur Lösung der Aufgabe besteht darin, die zu schützende Fläche eines Dokumentes untrennbar mit einem Schutzmuster zu versehen, das eine kodierte, über die gesamte zu schützende Fläche verspreizte Echtheitsinformation enthält. Als Echtheitsinformation eignen sich dabei beliebige alfanumerische Texte. Erfindungsgemäß wird die Kodierung der Echtheitsinformation und ihre Verspreizung über die zu schützende Fläche dadurch erreicht, daß die einzelnen alfanumerischen Zeichen zunächst durch die Symbole eines zwei- oder mehrwertigen Kodes ersetzt werden. Dabei ist aus der Nachrichtentechnik bekannt, daß sich mit einem n-stelligen und m-wertigen Kode $N = m^n$ verschiedene Zeichen darstellen lassen. Mit Hilfe eines sechstelligen Binärkodes lassen sich so zum Beispiel insgesamt $N = 2^6 = 64$ verschiedene Buchstaben, Ziffern und Sonderzeichen kodieren, so daß jedes dieser Zeichen durch $n = 6$ binäre Symbole dargestellt wird. Jedem der m verschiedenen

Kodesymbole wird nun eines von m unterschiedlichen Flächenmustern zugeordnet, die als optische Trägersignale für die entsprechenden Kodesymbole verwendet werden. Jedes alfanumerische Zeichen oder Sonderzeichen kann somit durch n flächig angeordnete Flächenmuster repräsentiert werden. Besteht die im Schutzmuster zu kodierende Echtheitsinformation aus k alfanumerischen Zeichen, so ergibt sich durch systematische Anordnung der einzelnen, die Kodesymbole repräsentierenden Flächenmuster ein zusammenhängendes Schutzmuster, das aus insgesamt k · n Flächenmustern aufgebaut ist.

Dem Erfindungsgedanken folgend wird nun vorgeschlagen, dieses Schutzmuster dem zu schützenden Dokument zu überlagern und es mit ihm auf geeignete Weise untrennbar zu verbinden. Die Helligkeitswerte von Dokument und Schutzmuster verbinden sich dabei zu einem optischen Gesamteindruck, der dem der bekannten Linienmuster ähnlich ist. Bei einer visuellen Prüfung auf Unverfälschtheit werden Manipulationen des Dokuments an Verletzungen des Schutzmusters und am veränderten optischen Gesamteindruck erkannt. Da das Schutzmuster nur aus wohldefinierten Grundelementen, nämlich den m unterschiedlichen Flächenmustern aufgebaut ist, läßt sich die im Schutzmuster kodierte Echtheitsinformation durch Unterscheidung der einzelnen Flächenmuster maschinell dekodieren. Ein bei einem Fälschungsversuch zerstörtes Flächenmuster führt zwangsläufig zu einer fehlerhaft dekodierten Echtheitsinformation, so daß die Manipulation maschinell selbst dann erkannt wird, wenn der optische Gesamteindruck des Dokuments unverdächtig erscheint.

Einzelheiten und weitere Eigenschaften der Erfindung werden im folgenden anhand der Zeichnungen erläutert.

Es zeigen

Fig. 1 einen Ausschnitt aus einem Dokument ohne erfindungsgemäßes Schutzmuster

Fig. 2 ein Ausführungsbeispiel eines erfindungsgemäßen Schutzmusters

Fig. 3 einen Ausschnitt aus einem Dokument, das durch ein erfindungsgemäßes Schutzmuster geschützt ist.

Fig. 4 - 9 verschiedene Beispiele für die die Kodesymbole repräsentierenden Flächenmuster

Fig. 10 eine Anordnung zur automatischen Echtheitsprüfung

Fig. 11 eine weitere Anordnung zur automatischen Echtheitsprüfung

Fig. 12 eine Anordnung zur Erzeugung von Dokumenten mit erfindungsgemäßem Schutzmuster

Fig. 1 zeigt einen Ausschnitt aus einem Dokument, das mit üblichen Fälschungsschutzmitteln wie Wasserzeichen, Metallfäden und dgl. versehen sein kann. Dabei ist auf einen Dokumententräger 1, der aus Kunststoff bestehen kann, vorzugsweise aber aus Papier bestehen soll, die das Dokument kennzeichnende Information in Form von Schriftzeichen oder sonstigen Markierungen aufgebracht. Diese Information besteht wenigstens zum Teil aus einer individuellen Information 2, die ein bestimmtes Dokument von anderen Dokumenten der gleichen Art unterscheidet, Bei Ausweisen sind dies vor allem die Ausweisnummer, personenbezogene Daten des Ausweisinhabers, sowie Ausgabestelle und Datum. In Fig. 1 besteht die individuelle Information 2 beispielsweise aus Schriftzeichen, die den Namen der Bank, die Konto- und die Checknummer bezeichnen. Vor allem diese individuelle Information ist fälschungsgefährdet und sollte vorzugsweise als Teil der Echtheitsinformation in das Schutzmuster einkodiert werden.Dies verhindert eine Fälschung der individuellen Information durch Hinzufügen von Klartextzeichen, da die Fälschung durch Vergleich mit der dekodierten Information des Schutzmusters erkannt wird.

In Fig. 2 ist ein erfindungsgemäßes Schutzmuster schematisch dargestellt. Es besteht beispielsweise aus der wiederholten Anordnung von 4 unterschiedlichen Flächenmustern 3, die die Symbole eines hier vierwertig angenommenen Kodes repräsentieren. Selbstverständlich sind auch beliebige andere Kodierungen inklusive kryptographischer Verschlüsselungen anwendbar. Zur Reduzierung des Aufwands bei der Herstellung und Prüfung des Schutzmusters wird vorzugsweise ein binärer Kode vorgeschlagen.

Die unterschiedlichen Flächenmuster sind in Fig. 2 durch unterschiedliche Schraffierungen gekennzeichnet und dabei so angeordnet, daß sie ein Schutzmuster bilden, das die gesamte zu schützende Dokumentenfläche bedeckt. Zusätzlich zu den Flächenmustern 3 werden Markierungen 4 vorgesehen, die zum Lesen und Dekodieren der im Schutzmuster enthaltenen Echtheitsinformationen benötigt werden.

Fig. 3 zeigt ein erfindungsgemäß geschütztes Dokument 5, bei dem die individuelle Information 2 Bestandteil der Echtheitsinformation ist und in kodierter Form über die Fläche des Schutzmusters verspreizt ist. Die untrennbare Verbindung von Dokument und Schutzmuster kann vorzugsweise durch Überdrucken des Dokuments geschehen. Eine andere Art der Verbindung zeigt Fig. 9 als stark vergrößerten Querschnitt durch ein Dokument. Auf einen Dokumententräger 1, auf den eine individuelle Information im Klartext aufgedruckt ist, wird mit Hilfe eines sehr agressiven Klebstoffes 10 eine dünne, transparente Kunststoffolie 9 aufgebracht, die vorher auf ihrer dem Dokument zugewandten Seite mit einem erfindungsgemäßen Schutzmuster bedruckt wurde. Durch Druck und Hitze läßt sich die Kunststoffolie 9 untrennbar mit dem Dokumententräger 1 verbinden.

Die Flächenmuster 3, aus denen das Schutzmuster gebildet wird, bestehen ihrerseits aus mindestens zwei Arten von Rasterelementen 6, 7 mit unterschiedlichen Reflexions- und / oder Transmissions- und / oder Fluoreszenzeigenschaften im sichtbaren und / oder unsichtbaren Teildes Lichtspektrums. So können zum Beispiel in sich mehrfarbige und verschieden strukturierte Flächenmuster erzeugt werden, die sowohl bei einer visuellen als auch bei einer maschinellen Echtheitsprüfung mit optischen Mitteln unterschieden werden können. Um die Sicherheit des Schutzmusters weiter zu vergrößern, lassen sich zusätzlich andere Prüfmethoden anwenden. So können zum Beispiel unterschiedliche Flächenmuster 3, die unterschiedlichen Kodesymbolen entsprechen, durch Zusätze zur Druckfarbe auch magnetisch unterscheidbar gemacht werden. Hierdurch wird eine Nachahmung des Schutzmusters durch einen optischen Kopiervorgang verhindert.

In Fig. 4 bis Fig. 8 sind verschiedene Ausführungsbeispiele für die Flächenmuster 3 dargestellt. Die Begrenzungslinie einzelner Flächenmuster kann dabei beliebig verlaufen, sie kann z. B. quadratisch, rechteckig, sechseckig oder unregelmäßig wie in Fig. 7 sein. Zweckmäßig werden jedoch solche Begrenzungslinien bevorzugt, die ein lückenloses Aneinanderfügen der Flächenmuster ermöglichen. Ebenso sind die Form und Größe der mindestens zwei Arten von unterschiedlichen Rasterelementen 6, 7 beliebig.

Sind die Schriftzeichen, Markierungen und bildlichen Darstellungen eines Dokuments ebenfalls gerastert, so können die Rasterelemente 6, 7 der Flächenmuster 3 auf beliebige Weise mit den Rasterelementen der Schriftzeichen, Markierungen und bildlichen Darstellungen verschachtelt sein, wie dies an einem Beispiel in Fig. 8 gezeigt ist. Die Rasterelemente 6, 7 können aber auch direkt dem Druckbild der Schriftzeichen, Markierungen und bildlichen Darstellungen überlagert werden. Dabei werden die Helligkeitswerte des ursprünglichen Druckbildes verändert. Um Verdeckungen des Druckbildes zu vermeiden, müssen Helligkeitswerte, Größe und Form der Rasterelemente dem zu schützenden Dokument angepaßt werden.

Zur Kodierung der Echtheitsinformation besonders geeignete Flächenmuster 3 sind gewisse, orthogonale Karhunen-Loève Basisfunktionen, die man durch eine Karhunen-Loève Orthogonalzerlegung des zu schützenden Dokuments gewinnt. Die Theorie der Orthogonalzerlegung von Funktionen ist aus der Mathematik bekannt und wird in der Nachrichtentechnik auf Signale angewendet. Einzelheiten zu einer derartigen Anpassung der Flächenmuster 3 an die zu schützenden Dokumente sind in dem Artikel " A Signal Theoretic Method for Creating Forgery Proof Documents for Automatic Verification", Proceedings of Carnahan Conference on Crime Countermeasures, University of Kentucky, Lexington, 16. - 18. Mai 1979, Seite 101 - 109, zu finden.

Die Verwendung von gewissen, schachbrettartigen Karhunen-Loève Basisfunktionen ermöglicht wegen der Orthogonalität der Basisfunktionen einerseits eine optimale Unterscheidbarkeit unterschied-

licher Flächenmuster und gewährleistet eine besonders störunempfindliche Rückgewinnung der im Schutzmuster enthaltenen Echtheitsinformation. Ähnliche Ergebnisse werden durch die Verwendung von schachbrettartigen Walsh-Funktionen als Flächenmuster 3 erzielt.

Fig. 12 stellt eine Anordnung dar, mit der die für ein Dokument optimalen Flächenmuster bestimmt und ein Dokument mit dem erfindungsgemäßen Schutzmuster versehen werden kann. Der Dokumententräger 1 wird zusammen mit der zu schützenden individuellen Information 2 durch ein optisches System 11 und einen opto-elektrischen Wandler 12 z. B. zeilenweise abgetastet. Die den Helligkeitswerten entsprechenden elektrischen Signale werden durch den Analog-Digital-Umsetzer 13 digitalisiert und mit Hilfe des Digitalrechners 14 in orthogonale Karhunen-Loève Basisfunktionen zerlegt. Als geeignete Flächenmuster werden die Basisfunktionen ausgewählt, deren Zerlegungskoeffizienten die geringsten Varianzen besitzen. Eine als alfanumerischer Text über die Tastatur 25 eingegebene Echtheitsinformation wird durch den Digitalrechner 14 nach einem vorgegebenen Kode, z. B. binär, kodiert. Die Kodesymbole der so kodierten Echtheitsinformation werden vom Digitalrechner anschließend durch die ausgewählten Flächenmuster ersetzt und den digital gespeicherten Helligkeitswerten des ursprünglichen Dokuments zusammen mit einer Lesemarkierung 4 überlagert. Nach einer Digital-Analog-Umsetzung kann das erfindungsgemäß geschützte Dokument von einem elektro-optischen Wandler 24 entweder auf einen lichtempfindlichen Dokumententräger oder auf eine Druckmatrize aufgezeichnet werden. Eine mögliche Anwendung für die Anordnung der Fig. 12 liegt beispielsweise darin, ein Paßfoto mit einem Schutzmuster zu überlagern, das die personenbezogenen Daten des Ausweisinhabers in kodierter Form enthält. Ausweisfälschungen durch Austausch des Paßfotos werden so verhindert.

Fig. 10 zeigt eine Anordnung zur Echtheitsprüfung eines Dokumentes 5, das mit einem erfindungsgemäßen Schutzmuster versehen ist. Sie ist bis auf die Tastatur 25 und den elektro-optischen Wandler 24, an dessen Stelle die alfanumerische Anzeige 15 tritt, identisch.

Die Unterscheidung der den Kodesymbolen entsprechenden Flächenmuster erfolgt im Digitalrechner 14 mit Hilfe der Korrelationsdetektion, einem Verfahren, das aus der Nachrichtentechnik und der Mustererkennung bekannt ist. Hierbei wird die bereits erwähnte Markierung 4 zur Synchronisation des Abtasters verwendet. Nach der Dekodierung wird die im Schutzmuster enthaltene Information in der Anzeige 15 angezeigt. Fälschungen lassen sich durch Vergleich mit dem Klartextaufdruck des Dokuments erkennen.

Fig. 11 zeigt schematisch eine weitere Anordnung zur Echtheitsprüfung eines Dokumentes 5 mit Schutzmuster, die auf dem Prinzip der optischen Korrelation beruht. Zur Vereinfachung der Beschreibung sei angenommen, daß das Schutzmuster binär kodierte Daten enthält, die mit nur einem einzigen Flächenmuster dargestellt sind. Dieses Flächenmuster ist je nach Kodesymbol positiv oder negativ (invertiert)* im Schutzmuster enthalten. Das Dokument 5 befindet sich in der vorderen Brennebene der Linse 17 und wird durch eine kohärente Lichtquelle 16 beleuchtet. In der hinteren Brennebene der Linse 17 und gleichzeitig in der vorderen Brennebene der Linse 19 befindet sich ein Hologramm 18 des datentragenden Flächenmusters. Die in der hinteren Brennebene der Linse 19 auf einer Mattscheibe 21 entstehenden Helligkeitsverteilungen enthalten die Autokorrelation der Flächenmuster mit positiven oder negativen Vorzeichen. Um die binären Kodesymbole am Vorzeichen der Autokorrelation zu unterscheiden, wird die Mattscheibe gleichzeitig durch einen kohärenten Referenzstrahl 20 beleuchtet, der eine Auslöschung derjenigen Helligkeitsverteilungen bewirkt, die negativen Korrelationswerten entsprechen. Die hinter einer Lochblende 22 angebrachten Photodetektoren 23 wandeln die Hell-Dunkel-Verteilung in elektrische Signale, die von einem Analog-Digital-Umsetzer 13 digitalisiert und vom Digitalrechner 14 dekodiert und in der alfanumerischen Anzeige 15 angezeigt werden.

In der Erfindung wird ein neuartiges Schutzmuster angegeben, das einen ähnlichen Schutz vor Fälschung bietet, wie ein Hologramm, das jedoch im Gegensatz zu Hologrammen drucktechnisch auf einem Dokument angebracht werden kann und vielseitiger einsetzbar ist

* oder um 90° gedreht

als Hologramme. Das erfindungsgemäße Schutzmuster erlaubt außerdem eine visuelle Echtheitsprüfung und kann durch zusätzliche Maßnahmen wie magnetisch wirksame Druckfarben vor einer optischen Nachahmung geschützt werden. Es stellt somit eine wesentliche Erweiterung der bisher bekannten Methoden zum Fälschungsschutz von Dokumenten dar.

Nummer: 29 43 436
Int. Cl.³: G 06 K 19/06
Anmeldetag: 26. Oktober 1979
Offenlegungstag: 7. Mai 1981

2943436

P 29 43 436.4

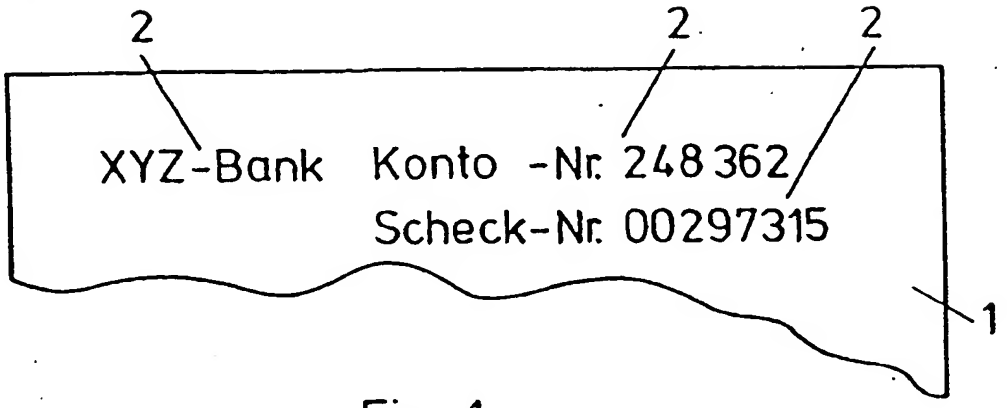

Fig.: 1

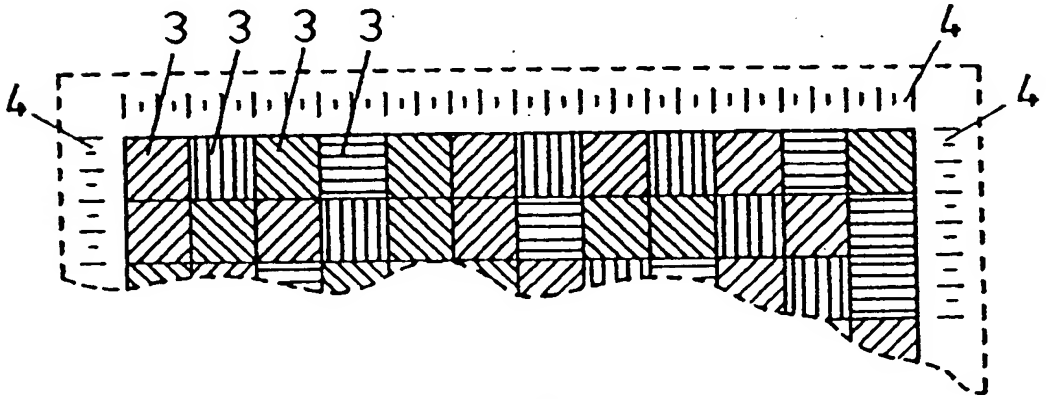

Fig.: 2

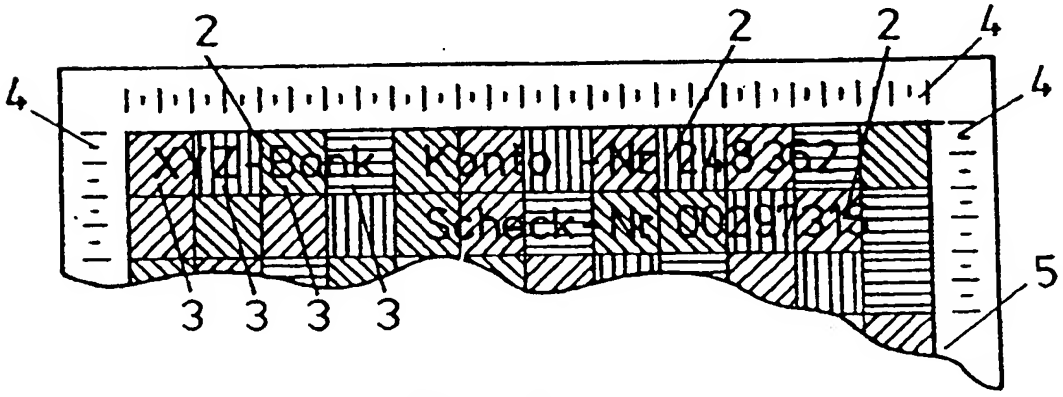

Fig.: 3

2943436

P 29 43 436.4

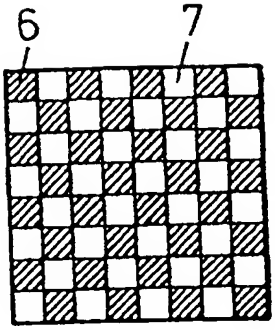

Fig.: 4

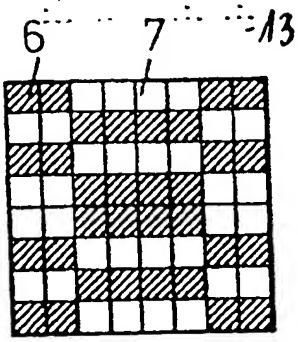

Fig.: 5

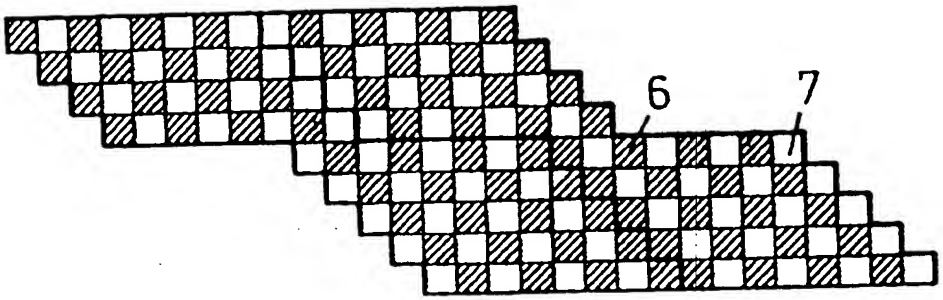

Fig.: 7

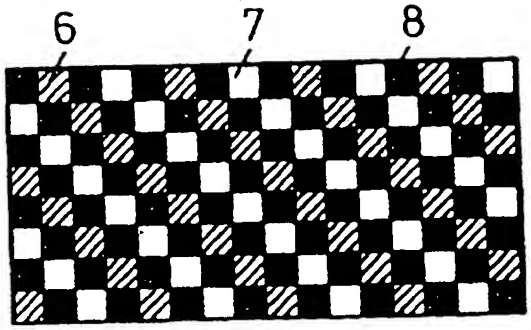

Fig.: 8

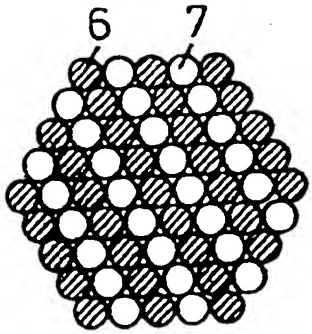

Fig.: 6

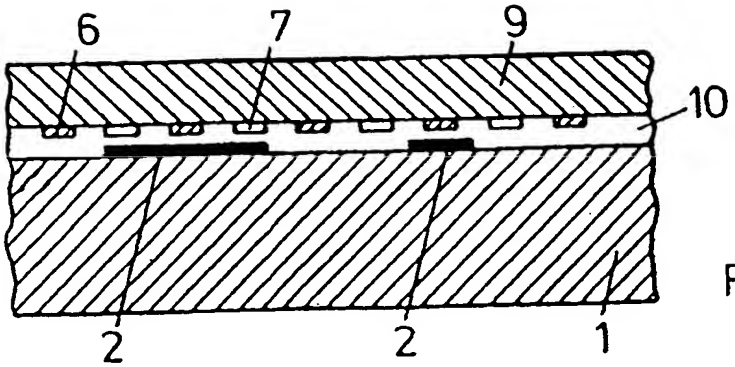

Fig.:9

2943436

P 29 43 436.4

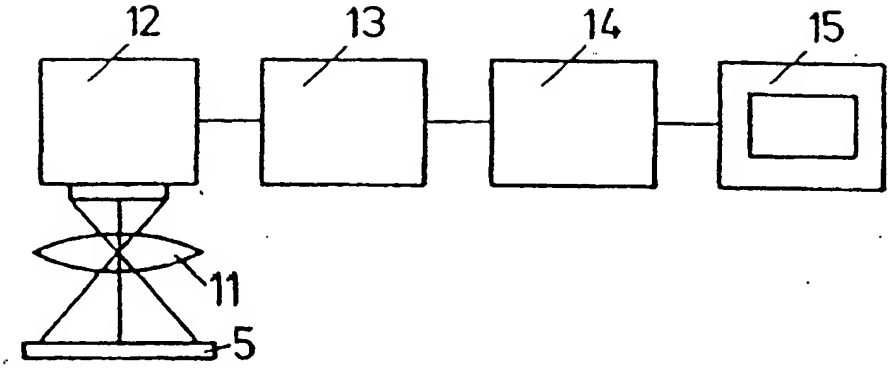

Fig.: 10

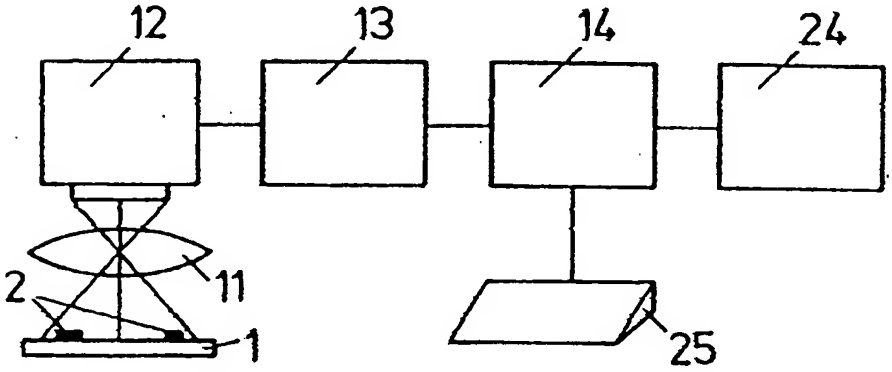

Fig.: 12

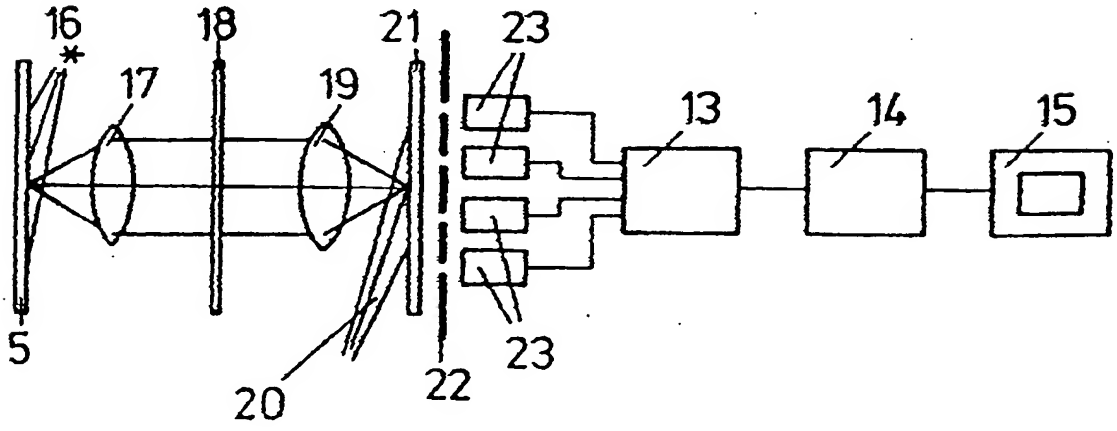

Fig.: 11

19. Federal Republic of Germany

German Patent Office

12. Unexamined application
11. DE 29 43 436 A1

51. Int. Cl.[3]: G 06K 19/06
G 07 C 9/00
G 07 D 7/00
B 44 F 1/12
B 41 M 3/14

21. Serial number: P 29 43 436.4-53
22. Date of filing: 10/26/79
43. Date of laying open for public inspection: 5/7/81

71. Applicant: Szepanski, Wolfram, Dr.-Ing. [Doctorate in Engineering], 5100 Aachen, Germany

72. Inventor: same as applicant

54. Machine testable security pattern for documents and procedure to create and test the security pattern

2943436

Patent Claims

1. Printable security pattern for forgery protection of documents that allows both visual and machine authenticity testing, characterized in that two-dimensionally distributed authenticity information is contained in the security pattern.

2. Security pattern according to claim 1, characterized in that the authenticity information consists of a coded alphanumeric text.

3. Security pattern according to claim 2, characterized in that the alphanumeric text consists entirely or partially of the individual information (2), by which two documents of the same type are differentiated.

4. Security pattern according to one of the claims 2 and 3, characterized in that the alphanumeric text is binary coded.

5. Security pattern according to one of the claims 1 through 4, characterized in that the distribution of the authenticity information is accomplished with adjacent two-dimensional patterns (3), which vary in their optical characteristics in the spectrum of visible and/or invisible light.

6. Security pattern according to one of the claims 1 through 5, characterized in that it is made up of orthogonal or bipolar two-dimensional patterns (3) that are different from each one another, particularly Walsh or Karhunen-Loève basis functions.

7. Security pattern according to one of the claims 1 through 6, characterized in that it is located on transparent plastic foil, which is applied to the surface of the document to be kept secure with aggressive glue under pressure and heat.

130019/0361

8. Security pattern according to one of the claims 1 through 6, characterized in that it is printed directly on the document to be kept secure.

9. Security pattern according to claim 8, characterized in that the document to be kept secure is a banknote, a check or a security.

10. Security pattern according to claim 7 and 8, characterized in that the document to be kept secure is a passport photo or an identity card.

11. Procedure for authenticity testing of the security pattern according to one of the claims 1 through 10 with the assistance of correlation detection, characterized in that the correlation is executed with a digital computer.

12. Procedure for authenticity testing of the security pattern according to one of the claims 1 through 10, characterized in that an arrangement is used for optical correlation.

13. Procedure for creation of a security pattern according to one of the claims 1 through 10, characterized in that a digital computer is used to modify the security pattern for the document and to produce the document itself or a print matrix for it.

Wolfram Szepanski, Dr.-Ing. [Doctorate in Engineering]
Harbachtalstrasse 21
5100 Aachen
Germany

Machine testable security pattern for documents and procedure to create and test the security pattern

---

The invention relates to a machine testable security pattern for documents, which contains authenticity information distributed over the surface of the document, as well as a procedure to create the security pattern and to test its authenticity.

In this case, the term "document" should be understood as passports, identity cards, authorization cards, credit cards, checks, banknotes, securities and similar items. Due to the wide dissemination of these documents and the value associated with them, various measures have already been taken to safeguard against imitations, erasures and other kinds of forgery. Documents whose authenticity characteristics are difficult to copy and forge and whose authenticity can be tested in different, independent ways and with little cost can be regarded as particularly secure. In doing so, forgery protection should preferably allow a simple visual authentication, but it should also be suited for a machine-based test with automatic reading devices, in order to enable a second, independent inspection independent from the visual inspection. Furthermore, documents that can be tested by machines are suitable as means of payment for vending machines or currency exchange machines, as identity cards for automatic access control etc. and everywhere where a large number of documents, such as banknotes or checks must be registered, sorted or counted by machine. The object of the invention is thus both a procedure to produce protected documents, as well as a procedure to test their authenticity by machine.

In order to make imitations more difficult and make forgeries easy to recognize, documents are frequently overlaid with a security pattern. The most commonly used are complicated line patterns (machine-turned backgrounds), which admittedly allow a visual authenticity test, but which are generally not machine-readable. The same applies to security patterns with a three-dimensional optical effect, to which no reference of any kind is made to machine testability in the printed specification of the application after examination (DE-AS 23 34 02) and/or the unexamined application (DT-OS 26 03 558).

In addition, procedures for document security are known, which are based upon the basic idea that certain machine-readable information or markings are applied to a document so they are invisible to a forger or hidden in the document. This can be attained, for example, by the use of materials with certain electric, magnetic or optical characteristics. This type of document protection cannot be tested without measuring equipment and also cannot be checked visually without additional measures. If, however, the existence of the invisible marking is recognized by a forger, there is a danger of forgery or imitation.

A protection against erasure is also proposed (DT-AS 25 30 905), in which the document is covered with a homogeneous, information-less protective layer, which differs in its optical characteristics from the information print color and from the paper and allows the attempts at erasure to be seen in a reading device. This procedure will not catch all the forgeries that are accomplished without erasures, for example, those where the name information or number values in the clear text on the document are changed by adding letters or numbers.

Creating documents that are very secure from forging by applying authenticity information to the document in the form of a hologram (DT-AS 25 01 604 and DT-AS 25 46 007) or an optical diffraction grid embossed in plastic (DT-AS 25 55 214) are also known. A difficult, unsolved problem

in doing so is the creation of scratch, fold and crumple-resistant holograms for checks and banknotes which are simultaneously, thin, highly flexible and durable for wear-resistance. Because the known holographically secure documents are either entirely or at least on their surface made of plastic, there can also be difficulties if the documents are to be later written upon or stamped. In addition, in the mass production of documents, the high production costs for holograms is disadvantageous.

Due to the cited deficiencies, the procedures for document security known to date are either not at all or not economically usable for certain types of documents or they only partially fulfill their security function. The objective of this invention is therefore to disclose a machine testable forgery protection for documents, which in a preferred embodiment also allows a visual authenticity test, and which can be used for all of the documents defined at the outset, without having the cited disadvantages of previously known security methods. It is also the objective of the invention to disclose procedures with which the production of the protection as well as its machine testing is possible.

The basic idea for attaining the objective lies in providing the surface of the document to be protected with an inseparable security pattern, which contains coded authenticity information distributed over the entire surface to be protected. In doing so, any alphanumeric text is suited as authenticity information. According to the invention, the coding of the authenticity information and its distribution over the surface to be protected is attained in that the individual alphanumeric characters are first replaced by the symbols of a code of two or more values. In doing so, it is known from telecommunications that with a n-digit and m-value code $N = m^n$ different characters can be displayed. Using a six-digit binary code, for example, it is thus possible to code a total of $N = 2^6 = 64$ different letters, numbers and special characters, so that each of these characters is shown through $n = 6$ binary symbols. Each of the m different

code symbols is now assigned one of m different surface patterns, which are used as optical carrier signals for the corresponding code symbols. Each alphanumeric character or special character can thus be represented with n 2-dimensionally arranged surface patterns. If the authenticity information to be coded in the security pattern consists of k alphanumeric characters, a systematic assignment of the individual, surface patterns representing code symbols results in a coherent security pattern that is made up of a total of $k \cdot n$ surface patterns.

According to the inventive idea, overlaying this security pattern on the document to be protected and inseparably bonding it with the document in an appropriate manner is now proposed. The brightness values of the document and security pattern combine in the process to an optical impression that is similar to the known line pattern. In a visual test for authenticity, the manipulations of the document will be recognized from damage to the security pattern and from a changed overall optical impression. Because the security pattern only consists of well-defined basic elements, namely the m different surface patterns, the authenticity information coded in the security pattern can be decoded by machine by differentiation of the individual surface patterns. A surface pattern destroyed during a forgery attempt automatically leads to incorrectly decoded authenticity information, so that the manipulation will even be recognized if the optical overall impression of the document seems unsuspicious.

Details and additional characteristics of the invention are explained in the following on the basis of the drawings.

They show:

Fig. 1 a section of a document without a security pattern according to the invention

Fig. 2 an embodiment of a security pattern according to the invention

Fig. 3 a section of a document that is protected with a security pattern according to the invention.

Fig. 4-9 different examples of the surface patterns which represent the code symbols

Fig. 10 an arrangement for automatic authenticity testing

Fig. 11 an additional arrangement for automatic authenticity testing

Fig. 12 an arrangement to create documents with a security pattern according to the invention

Fig. 1 shows a section of a document that can be provided with standard forgery security measures such as watermarks, metal threads and the like. In doing so, the information that identifies the document in the form of written characters or other markings is applied to a document carrier 1 that can consist of plastic, but preferably should consist of paper. This information consists at least in part of individual information 2, which differentiates a particular document from other documents of the same type. For identity cards this is primarily the identity number, personal data of the bearer of the identity card, as well as the place of issue and date. In Fig. 1, the individual information 2 consists for example of written characters that indicate the name of the bank, the account number and check number. This individual information, above all, is vulnerable to forgery and should preferably be encoded in the security pattern as part of the authenticity information. This prevents a forgery of the individual information by adding clear text characters because the forgery would be recognized by comparison with the decoded information of the security pattern.

Fig. 2 schematically shows a security pattern according to the invention. It consists, for example, of the repeated arrangement of 4 different surface patterns 3, which represent the symbols of a four-value code adopted in this case. Of course, any other codes can also be used, including cryptographic encoding. To reduce the expense in producing and testing the security pattern, a binary coded is preferably proposed.

In Fig. 2, the different surface patterns are characterized by different hatching patterns that are arranged in such a way that they form a security pattern, covering the entire document surface to be protected. In addition to the surface patterns 3, markings 4 are provided which are necessary for reading and decoding the authenticity information contained in the security pattern.

Fig. 3 shows a document 5 protected according to the invention in which the individual information 2 is part of the authenticity information and is distributed over the surface of the security pattern in coded form. The inseparable connection of document and security pattern can preferably occur by overprinting the document. Another type of connection is shown in Fig. 9 as a greatly enlarged cross-section of a document. A thin, transparent plastic foil 9 that is pre-printed with a security pattern according to the invention on the side facing the document is applied with a very aggressive glue 10 to a document carrier 1 on which individual information is printed in clear text. The plastic foil 9 can be bonded inseparably with the document carrier 1 using pressure and heat.

The surface pattern 3, from which the security pattern is formed, is itself comprised of at least two types of grid elements 6, 7 with different reflection and/or transmission and/or fluorescence properties in the visible and/or invisible range of the light spectrum. Thus, for example, a multicolored and variously structured surface pattern can be created, that can be differentiated with optical means in a visual and a machine authenticity test. To further increase the security of the security pattern, other test methods can also be used. For example, different surface patterns 3, which correspond to different code symbols, can also be made differentiable in a magnetic matter by additions to the printing ink. This prevents an imitation of the security pattern by an optical copying process.

In Fig. 4 through Fig. 8 there are different embodiments for the surface pattern 3 shown. The borderline of individual surface patterns can run as desired, it can, for example, be square, rectangular, hexagonal or irregular as shown in Fig. 7. Functionally, however, those borderlines that allow seamless, adjacent placement of the surface patterns are preferred. The shape and size of at least two types of different grid elements 6, 7 are also arbitrary.

If the written characters, markings and pictorial representations of a document are also in a grid, the grid elements 6, 7 of the surface pattern 3 can be encapsulated as desired with the grid elements of the written characters, markings and pictorial representations, as shown in an example in Fig. 8. The grid elements 6, 7 can also be overlaid directly on the print image of the written characters, markings and pictorial representations. In doing so, the brightness values of the original print image are changed. To avoid covering the print image, brightness values, size and shape of the grid elements must be adapted for the document to be protected.

Certain, orthogonal Karhunen-Loève basis functions that one attains by a Karhunen-Loève orthogonal decomposition of the document to be protected are surface patterns 3 are that are particularly suited for coding the authenticity information. The theory of the orthogonal decomposition of functions is known from mathematics and is used in telecommunications for signals. Details regarding this type of adaptation of the surface pattern 3 to the documents to be protected are found in the article, "A Signal Theoretic Method for Creating Forgery Proof Documents for Automatic Verification", Proceedings of Carnahan Conference on Crime Countermeasures, University of Kentucky, Lexington, May 16-18, 1979, Page 101-109.

The use of certain, checkered Karhunen-Loève basis functions enables optimal differentiation of different surface patterns due to the orthogonality of the basis function,

and guarantees a particularly interference-resistant recovery of the authenticity information contained in the security pattern. Similar results are attained by using checkered Walsh functions as surface patterns 3.

Fig. 12 shows an arrangement with which the optimal surface patterns for a document can be determined and a document can be provided with the security pattern according to the invention. The document carrier 1 is scanned line by line by an optical system 11 and an opto-electrical converter 12, for example, together with the individual information to be protected 2. The electrical signals corresponding to the brightness values are digitized by the analog-digital converter 13 and decomposed into orthogonal Karhunen-Loève basis functions using the digital computer 14. The basis functions that have decomposition coefficients with the lowest variances are selected as appropriate. Authenticity information input as alphanumeric text using the keyboard 25 is encoded by the digital computer 14 according to a given code, for example, binary. The code symbols of the authenticity information so encoded are then replaced by the digital computer with the selected surface pattern and the digitally saved brightness values of the original documents are overlaid together with a read marking 4. After a digital-analog conversion, the document protected according to the invention can either be transferred by an electro-optical converter 24 to a light-sensitive document carrier or to a print matrix. A possible use for the arrangement in Fig. 12 lies for example in overlaying a passport photo with a protective pattern that contains the personal data of the bearer of the identity card in coded form. This prevents identity card forgeries by exchanging the passport photo.

Fig. 10 shows an arrangement for authenticity testing of a document 5 that is provided with a protective pattern according to the invention. It is identical except for the keyboard 25 and the electro-optical converter 24, which is replaced by the alphanumeric display 15.

The differentiation of the surface patterns corresponding to the code symbols is accomplished in the digital computer 14 using the correlation detection, a procedure known from telecommunications and pattern recognition. In doing so, the already mentioned marking 4 is used to synchronize the scanner. After decoding, the information contained in the security pattern is shown on the display 15. Forgeries can be recognized by a comparison with the clear text printing on the document.

Fig. 11 schematically shows an additional embodiment for authenticity testing of a document 5 with a security pattern based upon the principle of optical correlation. To simplify the explanation, it is assumed that the security pattern contains binary coded data that is only shown with one single surface pattern. Depending upon the code symbol, this surface pattern is contained in the security pattern positively or negatively (inverted) or rotated 90 degrees. The document 5 is at the front focal plane of the lens 17 and is illuminated by a coherent light source 16. There is a hologram 18 of the data-carrying surface pattern in the back focal plane of the lens 17 and at the same time in the front focal plane of the lens 19. The brightness distributions generated on a matte disk 21in the back focal plane of lens 19 contain the auto correlation of the surface pattern with positive or negative operational signs. In order to differentiate the binary code symbols using the operational sign of the auto correlation, the matte disk is simultaneously illuminated by a coherent reference beam 20, which causes the brightness distributions corresponding to the negative correlation values to be extinguished. The photo detectors 23 mounted behind an aperture 22 convert the light-dark distribution into electric signals that are digitized by an analog-digital converter 13 and decoded by the digital computer 14 and shown in the alphanumeric display 15.

A new type of security pattern is disclosed in the invention that offers protection against forgery similar to a hologram, but in contrast to holograms it can be printed on a document and used in more ways

than a hologram. The security pattern according to the invention also allows a visual authenticity test and can also be protected from optical imitation using additional measures such as magnetic-acting ink. Thus, it represents a significant expansion of the known methods for protecting documents from forgery.

130019/0361